

PCT/JP 00/07682

01.11.00

09/869515

JP 00/7682 日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

REC'D 17 NOV 2000

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

1999年11月5日

出願番号

Application Number:

平成11年特許願第314521号

出願人

Applicant(s):

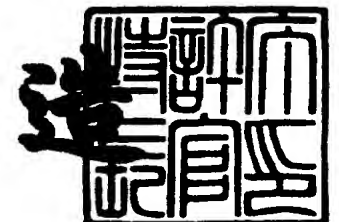
ソニー株式会社

BEST AVAILABLE COPY

2000年9月8日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3073091

【書類名】 特許願

【整理番号】 9900479603

【提出日】 平成11年11月 5日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

 【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

 【氏名】 赤池 正光

【特許出願人】

 【識別番号】 000002185

 【氏名又は名称】 ソニー株式会社

 【代表者】 出井 伸之

【代理人】

 【識別番号】 100082131

 【弁理士】

 【氏名又は名称】 稲本 義雄

 【電話番号】 03-3369-6479

【手数料の表示】

 【予納台帳番号】 032089

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

 【包括委任状番号】 9708842

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ処理装置およびデータ処理方法、並びに記録媒体

【特許請求の範囲】

【請求項 1】 データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理装置であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、前記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、

前記注目エントリに登録された前記エントリ有効情報に基づいて、前記注目エントリが有効かどうかを判定する判定手段と、

前記判定手段による判定結果に基づいて、前記データブロックに配置されたデータの出力を制御する出力制御手段と

を備えることを特徴とするデータ処理装置。

【請求項 2】 前記出力制御手段は、

前記注目エントリが有効である場合に、前記データを、前記データブロックに配置された宛先に出力し、

前記注目エントリが有効でない場合に、前記データを破棄することを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 3】 前記データは暗号化されており、

その暗号化されたデータを復号する復号手段をさらに備えることを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 4】 前記データは、そのデータの宛先に割り当てられた鍵を用いて暗号化されており、

前記テーブルの各エントリには、前記宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されており、

前記復号手段は、前記テーブルに登録されている前記鍵を用いて、前記データを復号する

ことを特徴とする請求項 3 に記載のデータ処理装置。

【請求項 5】 前記復号手段は、前記テーブルの、前記データブロックの宛先に割り当てられた前記鍵を用いて、そのデータブロックに配置されたデータを復号する

ことを特徴とする請求項 4 に記載のデータ処理装置。

【請求項 6】 前記テーブルの各エントリには、前記宛先、エントリ有効情報、および鍵の他、その鍵が有効かどうかを表す鍵有効情報も登録されており、前記復号手段は、

前記データブロックの宛先に割り当てられた前記鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定し、

有効である場合に、前記鍵を用いて、データを復号する

ことを特徴とする請求項 5 に記載のデータ処理装置。

【請求項 7】 前記テーブルの各エントリには、前記宛先およびエントリ有効情報の他、その宛先に割り当てられた 2 以上の鍵が登録されている

ことを特徴とする請求項 4 に記載のデータ処理装置。

【請求項 8】 前記テーブルの各エントリには、前記 2 以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報が登録されている

ことを特徴とする請求項 7 に記載のデータ処理装置。

【請求項 9】 前記テーブルを記憶するテーブル記憶手段をさらに備えることを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 10】 前記宛先は、前記データを受信すべき通信端末の MAC (Media Access Control) アドレスである

ことを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 11】 前記データブロックは、DVB (Digital Video Broadcasting) の規格に準拠したものである

ことを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 12】 1 チップの IC (Integrated Circuit) で構成されることを特徴とする請求項 1 に記載のデータ処理装置。

【請求項 13】 データとともに、そのデータの宛先が配置されたデータブロックを処理するデータ処理方法であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、前記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、

前記注目エントリに登録された前記エントリ有効情報に基づいて、前記注目エントリが有効かどうかを判定する判定ステップと、

前記判定ステップによる判定結果に基づいて、前記データブロックに配置されたデータの出力を制御する出力制御ステップと

を備えることを特徴とするデータ処理方法。

【請求項 1 4】 データとともに、そのデータの宛先が配置されたデータブロックを、コンピュータに処理させるプログラムが記録されている記録媒体であって、

宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、前記データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、

前記注目エントリに登録された前記エントリ有効情報に基づいて、前記注目エントリが有効かどうかを判定する判定ステップと、

前記判定ステップによる判定結果に基づいて、前記データブロックに配置されたデータの出力を制御する出力制御ステップと

を備えるプログラムが記録されている

ことを特徴とする記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、データ処理装置およびデータ処理方法、並びに記録媒体に関し、特に、例えば、データを、衛星回線等によって同報する場合に、そのデータを取得することのできる端末（ユーザ）を、容易に制限することができるようにするデータ処理装置およびデータ処理方法、並びに記録媒体に関する。

【0 0 0 2】

【従来の技術】

例えば、画像や音声等をデジタルデータで伝送する場合には、アナログ信号で伝送する場合と同一の伝送帯域で複数チャンネルを確保したり、また、より高品質の画像や音声を提供することが可能であり、衛星放送あるいは衛星通信等の分野では、画像や音声をデジタルデータで提供するシステムの普及が進んでいる。例えば、国内ではSkyPerfectTV!やDirecTV、北米ではDirecTV、欧州ではCanal Plus、といったデジタル衛星放送サービスが、それぞれ開始されている。放送のデジタル化は、1チャンネル当たりの送信コストの低減や、コンピュータで扱われるプログラムやデータの提供等を可能とし、また、デジタル化により、プログラム等と画像等とを連動して提供するようなサービスも普及しつつある。

【0 0 0 3】

デジタル衛星放送サービスでは、画像や音声のデジタルデータが、MPEG (Moving Picture Experts Group) 2や、このMPEG 2から派生したDVB (Digital Video Broadcasting)の規格に準拠したフォーマットに変換され、さらに多重化されて、電波として送信される。電波は、衛星のトランスポンダで受信され、増幅その他の必要な処理が施された後、地上に向けて送出される。

【0 0 0 4】

トランスポンダの伝送帯域は、例えば、30Mbps (Mega bit per second)と大きく（但し、トランスポンダでは、一般に、エラー訂正符号が付加されるので、30Mbpsの伝送帯域を有していても、実質的な伝送帯域は、最大で27Mbps程度）、このような大きな伝送帯域の全部を利用することで、デジタルデータを、高品位で、かつ高速に配信することが可能である。

【0 0 0 5】

しかしながら、一般には、主に、コスト上の理由から、トランスポンダの伝送帯域は、多チャンネルに分割されて使用されることが多い。この場合、各チャンネルで伝送されるデジタルデータの内容は異なっているとしても、各チャンネルのデジタルデータを受信する受信側の仕組みは共通であるため、あるデジタルデ

ータの提供を、特定のユーザだけが受けることができるような限定受信（CA (Conditional Access)）機構が必要となる。

【0006】

即ち、特に、例えば、いわゆるデータ放送を行う場合には、画像や音声を配信する場合に比較して、1番組当たりのデータ量が小さく、課金単位あるいは課金形態が複雑になることが予想され、これに対処するには、より細かな受信制御を行うことができる限定受信機構が必要となる。また、限定受信機構は、機密情報を配信する場合にも、その漏洩を防止するために必要となる。

【0007】

一般に、限定受信機構は、配信するデータストリームに対して暗号化を施すことによって実現される。暗号化方式としては、大きく分けて、共通鍵暗号化方式（秘密鍵暗号化方式）と、公開鍵暗号化方式とが知られている。ディジタル衛星放送では、暗号化／復号の処理の負荷が、公開鍵暗号化方式に比較して軽いことから、共通鍵暗号化方式が用いられることが多い。

【0008】

共通鍵暗号化方式では、ある契約者Aに対して、暗号鍵と同一の、復号鍵となる符号列を何らかの方法で渡し、データが、暗号鍵で暗号化されて配信される。暗号化されたデータは、それから、暗号鍵（復号鍵）や元のデータを逆計算する等して類推することが困難なようになっており、従って、契約者でないユーザBは、暗号化されたデータを受信しても、それを、元のデータに正しく復元することはできない。また、契約者であるユーザAは、暗号化されたデータを、契約することにより渡された復号鍵で復号することにより、元のデータを復元することができる。従って、受信契約とは、復号鍵の引き渡しを行うことと等価である。

【0009】

【発明が解決しようとする課題】

ところで、例えば、いま、ユーザAとCが契約者である場合において、ユーザAだけとの契約が終了したり、あるいは、ユーザAが不正な行為をしたときには、いままで使用していた暗号鍵を変更し、その変更後の暗号鍵と同一の復号鍵を、ユーザCのみに提供すれば、その後は、契約者でなくなった、あるいは不正な

行為を行ったユーザAは、新たな暗号鍵で暗号化されたデータを復元することができなくなるとともに、正当な契約者であるユーザCは、続けて、新たな暗号鍵で暗号化されたデータを、新たな復号鍵で復号することにより正常に復元することができる。

【0010】

しかしながら、あるユーザの契約が終了したり、不正な行為を発見するごとに、暗号鍵を変更し、さらに、変更後の暗号鍵と同一の復号鍵を、正当な契約者に提供するの面倒である。

【0011】

本発明は、このような状況に鑑みてなされたものであり、データを正常に取得する（受信する）ことのできるユーザを、容易に制限することができるようにするものである。

【0012】

【課題を解決するための手段】

本発明のデータ処理装置は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索手段と、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定手段と、判定手段による判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御手段とを備えることを特徴とする。

【0013】

出力制御手段には、注目エントリが有効である場合に、データを、データブロックに配置された宛先に出力させ、注目エントリが有効でない場合に、データを破棄させることができる。

【0014】

データが暗号化されている場合には、データ処理装置には、暗号化されたデータを復号する復号手段をさらに設けることができる。

【0015】

データが、そのデータの宛先に割り当てられた鍵を用いて暗号化され、テーブルの各エントリに、宛先およびエントリ有効情報の他、その宛先に割り当てられた鍵も登録されている場合には、復号手段には、テーブルに登録されている鍵を用いて、データを復号させることができる。

【0016】

復号手段には、テーブルの、データブロックの宛先に割り当てられた鍵を用いて、そのデータブロックに配置されたデータを復号させることができる。

【0017】

テーブルの各エントリに、宛先、エントリ有効情報、および鍵の他、その鍵が有効かどうかを表す鍵有効情報も登録されている場合には、復号手段には、データブロックの宛先に割り当てられた鍵の鍵有効情報に基づいて、その鍵が有効かどうかを判定させ、有効であるときに、鍵を用いて、データを復号させることができる。

【0018】

テーブルの各エントリには、宛先およびエントリ有効情報の他、その宛先に割り当てられた2以上の鍵も登録することができる。

【0019】

テーブルの各エントリには、2以上鍵それぞれについて、その鍵が有効かどうかを表す鍵有効情報も登録することができる。

【0020】

本発明のデータ処理装置には、テーブルを記憶するテーブル記憶手段をさらに設けることができる。

【0021】

宛先は、データを受信すべき通信端末のMAC(Media Access Control)アドレスとすることができる。

【0022】

データブロックは、DVB(Digital Video Broadcasting)の規格に準拠したものとすることができる。

【0023】

本発明のデータ処理装置は、1チップのIC(Integrated Circuit)で構成することができる。

【0024】

本発明のデータ処理方法は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えることを特徴とする。

【0025】

本発明の記録媒体は、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照し、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリを、注目エントリとして検索する検索ステップと、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうかを判定する判定ステップと、判定ステップによる判定結果に基づいて、データブロックに配置されたデータの出力を制御する出力制御ステップとを備えるプログラムが記録されていることを特徴とする。

【0026】

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体においては、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうか判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。

【0027】

【発明の実施の形態】

図1は、本発明を適用した放送システム（システムとは、複数の装置が論理的に集合した物をいい、各構成の装置が同一筐体中にあるか否かは問わない）の一実施の形態の構成例を示している。

【0028】

図1の実施の形態においては、放送システムは、送信システム1、衛星2、受信システム3、およびネットワーク4から構成されている。なお、図1では、図が煩雑になるのを避けるため、1の受信システム（受信システム3）しか図示していないが、受信システムは、2以上設けることが可能である。

【0029】

送信システム1は、制御装置11、データサーバ12、送信処理装置13、アンテナ14、回線接続装置15、およびケーブル16で構成され、制御装置11、データサーバ12、送信処理装置13、および回線接続装置15は、ケーブル16を介して相互に接続されることで、LAN (Local Area Network) を構成している。

【0030】

制御装置11は、データサーバ12を制御することにより、送信処理装置13に対して、衛星放送で配信すべきデータを供給させる。また、制御装置11は、回線接続装置15を制御することにより、インターネット等の外部のネットワーク4から、衛星放送で配信すべきデータを取得させ、送信処理装置13に対して供給させる。さらに、制御装置11は、送信処理装置13における各種の処理を制御する。

【0031】

データサーバ12は、衛星放送で配信すべきデータを記憶しており、制御装置11の制御にしたがって、必要なデータを、送信処理装置13に供給する。

【0032】

送信処理装置13は、制御装置11の制御にしたがい、データサーバ12や回線接続装置15から供給されるデータを、例えば、IP (Internet Protocol) パケットにパケット化し、さらに、そのIPパケットを、DVBデータ放送仕様に

準拠したセクション、即ち、例えば、EN 301 192 V1.1.1(1997-12), DVB specification for data broadcasting ETSI(European Telecommunications Standards Institute)で規定されているマルチプロトコルエンキャプスレイション(Multiprotocol Encapsulation)に基づくディスクリプタで記述されたセクションと呼ばれるデータブロックにブロック化する。そして、送信処理装置 1 3 は、セクションを、所定長のペイロードに分割し、各ペイロードに、MPEG 2 のトランスポートストリームを構成するパケット（以下、適宜、TS(Transport Stream)パケットという）のヘッダを付加することで、TSパケットに類するパケットを構成し、さらに、変調、増幅等の必要な処理を施して、アンテナ 1 4 から、衛星放送波として送出する。

【0033】

また、送信処理装置 1 3 は、受信システム 3 を構成する端末 24_1 , 24_2 , ・ ・ ・ (図 1 において図示していない受信システムを構成する端末についても同様) それぞれのMACアドレスと、各MAC(Media Access Control)アドレスに割り当てた暗号鍵とを対応付けた表形式の暗号鍵テーブルを記憶している暗号鍵テーブル記憶部 1 3 A を有している。なお、各MACアドレスに割り当てる暗号鍵は、基本的には、すべて異なるものとする。但し、一部のMACアドレスについて、同一の暗号鍵を割り当てるようにしても良い。

【0034】

ここで、MACアドレスとは、IEEE(Institute of Electrical Electronics Engineers) 802. 3等に適用されるアドレス体系であり、通信ポートごとに固有の48ビットの値で、重複がないことが保証されている。48ビットのMACアドレスは、その上位24ビットが、IEEEによって登録／管理される製造者(ベンダ(vendor)) 識別番号となっており、その下位24ビットが、各ベンダによって管理される機器識別番号となっている。MACアドレスによれば、受信システム 3 の各端末 24_i ($i = 1, 2, \dots$) を特定することができる。

【0035】

上述のマルチプロトコルエンキャプスレイションによれば、セクションのヘッダ(セクションヘッダ) には、そのセクションのペイロードに配置されたデータ

を配信する端末 2 4_i の宛先として、その端末の MAC アドレスが配置されるようになっている。セクションのパイロードに配置されるデータ、即ち、ここでは、IP パケットを暗号化する場合には、送信処理装置 1 3 は、セクションのヘッダに配置される宛先としての、端末 2 4_i の MAC アドレスに割り当てられた暗号鍵を、暗号鍵テーブル記憶部 1 3 A に記憶された暗号鍵テーブルから読み出し、その暗号鍵で、そのセクションのパイロードに配置される IP パケットを暗号化している。

【0 0 3 6】

なお、暗号鍵テーブルは、受信システム 3 を構成する、後述する受信装置 2 2 が有する鍵テーブルと同一形式のものであっても良いし、異なる形式のものであっても良い。また、ここでは、暗号鍵テーブルを、送信システム 1 に内蔵させておくようにしたが、暗号鍵テーブルは、例えば、ネットワーク 4 上の図示せぬサーバに記憶させておき、必要に応じて、回線接続装置 1 5 を介して読み出して使用するようにすることも可能である。

【0 0 3 7】

回線接続装置 1 5 は、例えば、モデムや、T A (Terminal Adapter) および D S U (Digital Service Unit) 等で構成され、ネットワーク 4 を介しての通信制御を行うようになっている。

【0 0 3 8】

受信システム 3 は、アンテナ 2 1、受信装置 2 2、回線接続装置 2 3、端末 2 4₁、2 4₂、・・・、およびケーブル 2 5 で構成されており、受信装置 2 2、回線接続装置 2 3、端末 2 4₁、2 4₂、・・・は、ケーブル 2 5 を介して相互に接続され、これにより、例えば、イーサネット（商標）等の LAN を構成している。

【0 0 3 9】

なお、受信装置 2 2 や、端末 2 4₁、2 4₂、・・・は、例えば、コンピュータで構成することができる。

【0 0 4 0】

また、ここでは、受信装置 2 2 と、端末 2 4₁、2 4₂、・・・とは、ケーブル

25で相互に接続することにより、LANを構成させるようにしたが、受信装置22と、端末24₁、24₂、・・・とは、直接接続するようにすることも可能である。

【0041】

さらに、受信装置22は、1台の端末24_iとしてのコンピュータのスロットに装着可能なボードとして構成することが可能である。

【0042】

また、受信装置22と回線接続装置23とは、1台のコンピュータで構成することが可能である。

【0043】

衛星2を介して、送信システム1から送信されてくる衛星放送波は、アンテナ21で受信され、その受信信号は、受信装置22に供給される。受信装置22は、アンテナ21からの受信信号に対して、後述するような処理を施し、その結果得られるデータを、所定の端末24_iに供給する。

【0044】

回線接続装置23は、回線接続装置15と同様に構成され、ネットワーク4を介しての通信制御を行うようになっている。

【0045】

端末24₁、24₂、・・・は、例えば、コンピュータで構成され、受信装置22から必要なデータを受信して、表示、出力、あるいは記憶等するようになっている。

【0046】

次に、図2のフローチャートを参照して、送信システム1が行うデータの送信処理について説明する。

【0047】

まず最初に、ステップS1において、制御装置11は、端末24_iに対して送信すべきデータがあるかどうかを判定する。

【0048】

ここで、制御装置11は、データを送信するスケジュールが記述されたスケジ

ユーラ表を有しており、そのスケジュール表に基づいて、端末 2 4_i に対して送信すべきデータがあるかどうかを判定する。また、端末 2 4_i は、回線接続装置 2 3 を制御することにより、ネットワーク 4 を介して、送信システム 1 に対して、データを要求することができるようになっており、制御装置 1 1 は、そのような要求が、ネットワーク 4 を介して回線接続装置 1 5 で受信されたかどうかによって、端末 2 4_i に対して送信すべきデータがあるかどうかを判定する。

【 0 0 4 9 】

ステップ S 1 において、端末 2 4_i に対して送信すべきデータがないと判定された場合、ステップ S 2 に進み、制御装置 1 1 は、期間を変更するかどうかを判定する。

【 0 0 5 0 】

ここで、送信システム 1 においては、暗号鍵テーブル記憶部 1 3 における暗号鍵テーブルに記述された暗号鍵が、定期的または不定期に更新されるようになっており、例えば、偶数回目の更新によって得られた暗号鍵を用いて暗号化が行われる期間が、Even 期間と呼ばれ、奇数回目の更新によって得られた暗号化器を用いて暗号化が行われる期間が、Odd 期間と呼ばれる。従って、Even 期間と Odd 期間とは交互に現れるが、ステップ S 2 では、Even 期間から Odd 期間に、または Odd 期間から Even 期間に変更する時期であるかどうか判定される。

【 0 0 5 1 】

ステップ S 2 において、期間を変更しないと判定された場合、即ち、いま暗号化に用いている暗号鍵をそのまま用いて、データの暗号化を続行する場合、ステップ S 1 に戻り、以下、上述の場合と同様の処理を繰り返す。

【 0 0 5 2 】

また、ステップ S 2 において、期間を変更すると判定された場合、即ち、いまが、Even 期間であるときには Odd 期間に、Odd 期間であるときには Even 期間に、期間を変更する場合、ステップ S 3 に進み、制御装置 1 1 は、暗号鍵テーブルに記憶された暗号鍵を、後述するステップ S 4 において前回生成された暗号鍵に更新し、これにより、その後は、送信処理装置 1 3 において、その更新された暗号鍵を用いて暗号化が行われる。

【 0 0 5 3 】

そして、ステップ S 4 に進み、制御装置 1 1 は、次の期間に用いる暗号鍵を生成し（あるいは取得し）、送信処理装置 1 3 に供給して、復号鍵として送信させ、ステップ S 1 に戻り、以下、上述の場合と同様の処理が繰り返される。なお、復号鍵の送信は、衛星 2 を介して行う他、ネットワーク 4 を介して行うことも可能である。

【 0 0 5 4 】

即ち、次の期間に用いる新たな復号鍵を、その、次の期間の開始直前に、受信システム 3 に送信したのでは、受信システム 3 において、新たな復号鍵の設定が、次の期間の開始までに間に合わないことがある。そこで、本実施の形態では、次の期間に用いる新たな暗号鍵は、その直前の期間において、受信システム 3 に対して配信されるようになっている。

【 0 0 5 5 】

一方、ステップ S 1 において、端末 2 4_i に対して送信すべきデータがあると判定された場合、制御装置 1 1 は、データサーバ 1 2 または回線接続装置 1 5 を制御することにより、その送信すべきデータを、送信処理装置 1 3 に供給させる。送信処理装置 1 3 は、データサーバ 1 2 または回線接続装置 1 5 から供給されるデータを受信し、IP パケットにパケット化して、ステップ S 5 に進む。

【 0 0 5 6 】

送信処理装置 1 3 は、ステップ S 5 において、IP パケットが、暗号化の必要なものであるかどうかを判定し、暗号化の必要なものでないと判定した場合、ステップ S 6 および S 7 をスキップして、ステップ S 8 に進む。

【 0 0 5 7 】

また、ステップ S 5 において、IP パケットが、暗号化の必要なものであると判定された場合、ステップ S 6 に進み、送信処理装置 1 3 は、その IP パケットの宛先となる端末 2 4_i の MAC アドレスに割り当てられた暗号鍵を、暗号鍵テーブルから読み出し、ステップ S 7 に進む。ステップ S 7 では、送信処理装置 1 3 は、IP パケットを、ステップ S 6 で読み出した暗号鍵で暗号化し、ステップ S 8 に進む。

【0058】

ステップS8では、送信処理装置は、IPパケットについてCRC (Cyclic Redundancy Checking)コード（あるいは、チェックサム）を演算し、そのIPパケットをペイロードとして、その最後に、CRCコードを配置するとともに、その先頭に、セクションヘッダを配置することで、図3（A）に示すようなセクションを構成する。なお、ペイロードとCRCコードとの間には、必要に応じて、スタッフィングバイトが挿入される。

【0059】

セクションヘッダは、図3（B）に示すように、3バイト（96ビット）で構成される。ここで、セクションヘッダの詳細については、上述のEN 301 192 V1.1.1(1997-12)に記載されているため、その説明は省略するが、図3（B）におけるMAC address 1乃至6に、宛先となる48ビットのMACアドレスが配置される。ここで、MAC address 1には、MACアドレスの最上位ビットから8ビットが配置され、MAC address 2には、その次の上位8ビットが配置される。そして、MAC address 3乃至5それぞれに、同様にしてMACアドレスが8ビットずつ配置され、MAC address 6には、MACアドレスの最下位の8ビットが配置される。

【0060】

送信処理装置13は、セクションを構成した後、そのセクションを、所定長のペイロードに分割し、各ペイロードに、MPEG2のトランスポートストリームを構成するTSパケットのヘッダを付加することで、TSパケットに類するパケットを構成するカプセル化を行う。そして、送信処理装置13は、ステップS9に進み、その結果得られるパケット（このパケットは、基本的には、TSパケットと同様に処理することができるので、以下、適宜、TSパケットという）に対して、変調、増幅等の必要な処理を施して、アンテナ14から、衛星放送波として送出し、ステップS1に戻る。

【0061】

なお、図3（B）に示したセクションヘッダにおいて、その先頭から43ビット目と44ビット目の2ビットに配置される2ビットのPSC(payload_scrambling_control)は、例えば、セクションのペイロードに配置されたデータが暗号化

されているかどうかを表す暗号化判定フラグ、およびそのデータが、Even期間またはOdd期間のうちのいずれの期間のものを表す期間判定フラグとして用いられるようになっている。

【0062】

具体的には、例えば、PSCの下位ビットは、暗号化判定フラグとして用いられ、データが暗号化されているときには1に、暗号化されていないときには0とされる。また、PSCの上位ビットは、期間判定フラグとして用いられ、Even期間では0に、Odd期間では1にされる。但し、PSCの上位ビットを、暗号化判定フラグとして用いるとともに、その下位ビットを、期間判定フラグとして用いることも可能である。また、暗号化判定フラグの0と1の割り当てや、期間判定フラグの0と1の割り当ては、上述した場合と逆にすることも可能である。

【0063】

ここで、DVBの規格であるEN 301 192 V1.1.1(1997-12)では、PSCが、00B（Bは、その前に配置された値が2進数であることを表す）の場合が、データが暗号化されていないことを表すこととなっており、従って、暗号化判定フラグは、データが暗号化されているときには1に、暗号化されていないときには0とする方が、DVBの規格に反しないこととなるので望ましい。

【0064】

以上のように、図1の放送システムでは、各端末24_iに固有のMACアドレスに割り当てられた暗号鍵で、データが暗号化されるので、各端末24_iごとの受信制御という、いわば究極の限定受信機構を実現することができる。

【0065】

なお、MACアドレス、あるいはIPアドレス等の受信側に固有の値に暗号鍵を割り当てて、きめ細かい受信制御を行う限定受信機構を実現する方法については、本件出願人が先に提案した、例えば、特開平10-215244号公報に、その詳細が開示されている。但し、わが国における通信衛星放送が、DVB-SI (Digital Video Broadcasting - Service Information / EN300 468)から派生した仕様に準拠している現状においては、上述したように、MACアドレスを用いるのが、その仕様に適合することとなる。

【 0 0 6 6 】

次に、図 4 は、図 1 の受信装置 2 2 の構成例を示している。

【 0 0 6 7 】

アンテナ 2 1 は、衛星 2 を介して、送信システム 1 から送信されてくる衛星放送波を受信し、その受信信号を、フロントエンド部 3 1 に出力する。フロントエンド部 3 1 は、CPU 3 4 の制御にしたがい、アンテナ 2 1 からの受信信号から所定のチャンネルの信号を選局し、さらに、その信号を、TS パケットのデジタルストリーム(IP_datagram_data_byte)に復調して、デマルチプレクサ 3 2 に出力する。デマルチプレクサ 3 2 は、CPU 3 4 の制御にしたがい、フロントエンド部 3 1 からのデジタルストリームから、所定の TS パケットを抽出し、復号 L S I (Large Scale Integrated Circuit) 3 3 に出力する。即ち、デマルチプレクサ 3 2 は、フロントエンド部 3 1 からのデジタルストリームを構成する TS パケットのヘッダに配置されている P I D (Packet Identification) に基づいて、TS パケットの取捨選択を行い、選択した TS パケットのみを、復号 L S I 3 3 に出力する。

【 0 0 6 8 】

復号 L S I 3 3 は、1 チップの L S I で、フィルタ 4 1、復号器 4 2、鍵テーブル記憶部 4 3、チェッカ 4 4、および F I F O (First In First Out) バッファ 4 5 で構成されている。

【 0 0 6 9 】

フィルタ 4 1 は、CPU 3 4 の制御にしたがい、デマルチプレクサ 3 2 からの TS パケットで構成されるセクションのペイロードに配置されたデータを、必要に応じて検査し、不必要な TS パケットを破棄し、必要な TS パケットだけを復号器 4 2 に出力する。

【 0 0 7 0 】

復号器 4 2 は、フィルタ 4 1 からの TS パケットで構成されるセクションのペイロードに配置されたデータ（ここでは、IP パケット）を、鍵テーブル記憶部 4 3 に記憶された復号鍵で復号し、チェッカ 4 4 に出力する。また、復号器 4 2 は、図 2 で説明したように、送信システム 1 において暗号鍵が更新され、その更

新された暗号鍵が送信されてきた場合、CPU 3 4 の制御にしたがい、その暗号鍵を、復号鍵として、鍵テーブル記憶部 4 3 の記憶内容を更新する。従って、ここでは、暗号化方式として、共通鍵暗号化方式が用いられるようになっている。但し、暗号化方式としては、公開鍵暗号化方式を用いることも可能である。

【 0 0 7 1 】

鍵テーブル記憶部 4 3 は、受信装置 2 2 にケーブル 2 5 を介して接続された端末 2 4₁, 2 4₂, … それぞれの MAC アドレスと、それぞれに割り当てられた復号鍵とが対応付けられて登録された鍵テーブルを記憶している。

【 0 0 7 2 】

チェッカ 4 4 は、CPU 3 4 の制御にしたがい、復号器 4 2 が出力する IP パケットについて、その IP パケットが配置されていたセクションの CRC コードを用いて誤り検出を行い、これにより、復号器 4 2 における復号が正常に行われたかどうか等を判定する。チェッカ 4 4 で処理された IP パケットは、F I F O バッファ 4 5 に供給されるようになっており、F I F O バッファ 4 5 は、チェッカ 4 4 からの IP パケットを一時記憶し、CPU 3 4 の制御にしたがい、記憶した IP パケットを、I / F (Interface) 3 5 に出力する。これにより、IP パケットのデータレートが調整される。

【 0 0 7 3 】

CPU 3 4 は、フロントエンド部 3 1、デマルチプレクサ 3 2、復号 L S I 3 3、および I / F 3 5 を制御する。I / F 3 5 は、CPU 3 4 の制御にしたがい、F I F O バッファ 4 5 からの IP パケットを、ケーブル 2 5 を介して、端末 2 4₁ に供給するインタフェースとして機能する。

【 0 0 7 4 】

次に、図 5 は、図 4 の鍵テーブル記憶部 4 3 に記憶されている鍵テーブルの構成例を示している。

【 0 0 7 5 】

鍵テーブルは、例えば、ケーブル 2 5 に接続されている端末 2 4₁, 2 4₂, … の数と同一数のエントリから構成されている。図 5 では、鍵テーブルは、N 個のエントリ # 1 乃至 # N を有しており、従って、本実施の形態では、ケーブル

25には、N個の端末 24_1 乃至 24_N が接続されている。なお、鍵テーブルのエントリの最大数は、鍵テーブル記憶部43の記憶容量等によって制限される。

【0076】

各エントリ# i ($i = 1, 2, \dots, N$)には、端末 24_i の48ビットのMACアドレスMACaddress# i と、そのMACアドレスに割り当てられた m ビットの復号鍵 (m は、使用する暗号形式による) とが対応付けられて登録されている。なお、本実施の形態では、上述したように、Even期間とOdd期間とが存在し、それぞれの期間では、異なる暗号鍵で暗号化が行われるため、各エントリ# i には、Even期間に暗号化されたデータを復号するための復号鍵 (以下、適宜、Even復号鍵という) $K_{\text{Even}\#i}$ と、Odd期間に暗号化されたデータを復号するための復号鍵 (以下、適宜、Odd復号鍵という) $K_{\text{Odd}\#i}$ との2つの復号鍵が登録されている。

【0077】

さらに、各エントリ# i のMACアドレスMACaddress# i の先頭には、そのエントリ# i が有効であるかどうかを表すValidビット (以下、適宜、エントリValidビットという) が付加されている。また、各エントリ# i のEven復号鍵 $K_{\text{Even}\#i}$ とOdd復号鍵 $K_{\text{Odd}\#i}$ にも、それぞれが有効かどうかを表すValidビット (以下、適宜、復号鍵Validビットという) が付加されている。

【0078】

ここで、エントリValidビット、復号鍵Validビットは、例えば、それが1の場合が有効であることを表し、0の場合が有効でないことを表す。但し、エントリValidビット、復号鍵Validビットの0と1の割り当ては、上述した場合と逆にすることも可能である。

【0079】

上述したように、送信システム1においては、次の期間に用いる新たな暗号鍵と同一の復号鍵は、その直前の期間に、受信システム3に対して配信されるようになっている。従って、Even期間においては、その次のOdd期間で用いられる暗号鍵と同一の復号鍵 (Odd復号鍵) が配信され、Odd期間においては、その次のEven期間で用いられる暗号鍵と同一の復号鍵 (Even復号鍵) が配信される。そして

、復号器 4 2 では、CPU 3 4 の制御の下、そのようにして配信されてくる復号鍵が、鍵テーブルに設定（例えば、上書き）される。従って、この場合、鍵テーブルには、次の期間に用いられる復号鍵が、現在の期間が終了するまでに設定され、さらに、期間の変更に伴う復号鍵の変更は、CPU 3 4 を介在せずに、復号器 4 2 が読み出しを行う鍵テーブルの位置（アドレス）を切り替えるだけで済むので、瞬時に行うことができる。

【 0 0 8 0 】

次に、図 6 のフローチャートを参照して、図 4 の受信装置 2 2 の動作について説明する。

【 0 0 8 1 】

アンテナ 2 1 では、衛星 2 を介して、送信システム 1 から送信されてくる衛星放送波が受信され、その結果得られる受信信号は、フロントエンド部 3 1 およびデマルチプレクサ 3 2 を介することにより、TS パケットのデジタルストリームとされ、復号 LSI 3 3 に供給される。

【 0 0 8 2 】

復号 LSI 3 3 では、デマルチプレクサ 3 2 が出力する TS パケットで構成されるセクションが、フィルタ 4 1 を介して、復号器 4 2 に供給される。復号器 4 2 は、セクションを受信し、ステップ S 1 1 において、そのセクションヘッダに配置された MAC アドレスを、内蔵するレジスタとしての変数 MA にセットする。

【 0 0 8 3 】

復号器 4 2 は、鍵テーブルを参照することにより、変数 MA に一致する MAC アドレスのエントリを検索し、即ち、鍵テーブルのエントリ # 1 から順に、各エントリ # i に登録されている MAC アドレスを読み出して、その MAC アドレスと、変数 MA とを比較（照合）し、ステップ S 1 2 において、変数 MA に一致する MAC アドレスのエントリが存在するかどうかを判定する。ステップ S 1 2 において、変数 MA に一致する MAC アドレスのエントリが存在しないと判定された場合、即ち、セクションヘッダに配置された MAC アドレスを有する端末が、ケーブル 2 5 上に接続されていない場合、ステップ S 1 3 に進み、復号器 4 2 は

、そこに供給されたセクションを破棄し、処理を終了する。

【0084】

また、ステップS12において、変数MAに一致するMACアドレスのエントリが存在すると判定された場合、そのエントリを注目エントリとして、ステップS14に進む。

【0085】

ステップS14では、復号器42は、注目エントリのエントリValidビットに基づいて、その注目エントリが有効であるかどうかを判定する。ステップS14において、注目エントリが有効でないと判定された場合、即ち、注目エントリのエントリValidビットが0である場合、ステップS13に進み、復号器42は、そこに供給されたセクションを破棄し、処理を終了する。

【0086】

従って、復号器42に供給されたセクションのセクションヘッダに配置されたMACアドレスを有する端末が、ケーブル25上に接続されている場合でも、そのMACアドレスのエントリが有効とされていないときには、そのセクションは、ケーブル25上の端末に供給されない。

【0087】

また、ステップS14において、注目エントリが有効であると判定された場合、即ち、注目エントリのエントリValidビットが1である場合、ステップS15に進み、復号器42は、セクションヘッダのPSC（図3（B））の下位ビット、即ち、暗号化判定フラグを参照し、セクションのペイロードのデータ（IPパケット）が暗号化されているかどうかを判定する。ステップS15において、暗号化判定フラグが0であると判定された場合、即ち、セクションのペイロードに配置されたIPパケットが暗号化されていない場合、ステップS17およびS18をスキップして、ステップS19に進み、復号器42は、その暗号化されていないIPパケットを、チェッカ44を介して、FIFOバッファ45に出力して、処理を終了する。

【0088】

そして、FIFOバッファ45に記憶されたIPパケットは、I/F35を介

して、その IP パケットが配置されていたセクションのセクションヘッダにおける MAC アドレスによって特定されるケーブル 2 5 上の端末 2 4_i に供給される。

【 0 0 8 9 】

一方、ステップ S 1 5 において、暗号化判定フラグが 1 であると判定された場合、即ち、セクションのペイロードに配置された IP パケットが暗号化されている場合、ステップ S 1 6 に進み、復号器 4 2 は、そのセクションのセクションヘッダの P S C (図 3 (B)) の上位ビット、即ち、期間判定フラグを、内蔵するレジスタとしての変数 E O にセットして、ステップ S 1 7 に進む。

【 0 0 9 0 】

ステップ S 1 7 では、復号器 4 2 は、MAC アドレスが変数 M A に一致する注目エントリにおける変数 E O に対応する期間、即ち、変数 E O が 0 である場合には Even 期間、1 である場合には Odd 期間の復号鍵の復号鍵 Valid ビット # (M A , E O) が有効であるかどうかを判定する。ステップ S 1 7 において、復号鍵 Valid ビット # (M A , E O) が有効でないと判定された場合、即ち、復号鍵 Valid ビット # (M A , E O) が 0 である場合、ステップ S 1 3 に進み、復号器 4 2 は、そこに供給されたセクションを破棄し、処理を終了する。

【 0 0 9 1 】

従って、復号器 4 2 に供給されたセクションのセクションヘッダに配置された MAC アドレスを有する端末が、ケーブル 2 5 上に接続されており、その MAC アドレスのエントリが有効とされている場合でも、期間判定フラグが表す期間の復号鍵が有効とされていないときには、そのセクションは、ケーブル 2 5 上の端末に供給されない。

【 0 0 9 2 】

一方、ステップ S 1 7 において、復号鍵 Valid フラグ # (M A , E O) が有効であると判定された場合、即ち、復号鍵 Valid ビット # (M A , E O) が 1 である場合、ステップ S 1 8 に進み、復号器 4 2 は、MAC アドレスが変数 M A に一致する注目エントリにおける、変数 E O に対応する期間の復号鍵 K e y (M A , E O) を、鍵テーブルから読み出し、その復号鍵 K e y (M A , E O) で、セク

ションのパイロードに配置された IP パケットを復号し、ステップ S 19 に進む。

【0093】

ステップ S 19 では、復号器 42 は、復号された IP パケットを、チェッカ 44 を介して、FIFO バッファ 45 に出力して、処理を終了する。

【0094】

そして、FIFO バッファ 45 に記憶された IP パケットは、I/F 35 を介して、その IP パケットが配置されていたセクションのセクションヘッダにおける MAC アドレスによって特定されるケーブル 25 上の端末 24_i に供給される。

【0095】

なお、図 6 のフローチャートにしたがった処理は、復号器 42 に対して、セクションが供給されるごとに行われる。

【0096】

以上のように、鍵テーブルのエントリに登録されたエントリ Valid ビットに基づいて、そのエントリが有効かどうかを判定し、端末に対するデータの出力を制御するようにしたので、データを正常に取得する（受信する）ことのできるユーザ（端末）を、容易に制限することが可能となる。

【0097】

さらに、鍵テーブルの復号鍵 Valid ビットにも基づいて、データの出力を制御するようにしたので、例えば、ある端末について、Even 期間または Odd 期間のうちのいずれか一方の期間のみのデータの受信を許可し、他方の期間のデータの受信を禁止することを、容易に行うことができる。

【0098】

なお、エントリ Valid ビットおよび復号鍵 Valid ビットの設定は、受信装置 22 において、いわば自主的に行うことも可能であるし、また、送信システム 1 から送信されてくる情報に基づいて行うことも可能である。

【0099】

また、本実施の形態では、復号鍵を（暗号鍵も）、端末に固有の MAC アドレ

スに割り当てるようにしたが、復号鍵は、その他、例えば、端末に固有の端末ID (Identification)を設定し、その端末IDに割り当てるようにすることも可能である。さらに、復号鍵は、複数の端末ごとに固有のグループIDを設定し、そのグループIDごとに割り当てるようにすることも可能である。但し、MACアドレスに対して復号鍵を割り当てる場合には、上述したようなきめの細かい限定受信機構を、DVBの規格であるEN 301 192 V1.1.1(1997-12)に準拠したデジタル衛星放送の枠組みに、容易に組み込むことが可能となる。

【0100】

また、本実施の形態では、フィルタ41、復号器42、鍵テーブル記憶部43、チェッカ44、およびFIFOバッファ45を、1チップの復号LSI33で構成するようにしたが、フィルタ41、復号器42、鍵テーブル記憶部43、チェッカ44、およびFIFOバッファ45は、それぞれ別のチップとして構成することも可能である。但し、フィルタ41、復号器42、鍵テーブル記憶部43、チェッカ44、およびFIFOバッファ45を、1チップの復号LSI33で構成した方が、データの復号が、復号LSI33の外部から完全に隠蔽された形で行われるため、セキュリティを向上させることができる。さらに、回路の実装面積の縮小や、処理の高速化等の観点からも、フィルタ41、復号器42、鍵テーブル記憶部43、チェッカ44、およびFIFOバッファ45は、1チップの復号LSI33で構成するのが望ましい。

【0101】

また、本実施の形態では、デジタル衛星放送によってデータを配信する場合について説明したが、本発明は、その他、例えば、マルチキャストでデータを配信する場合等にも適用可能である。

【0102】

さらに、本実施の形態では、Even期間とOdd期間の2つの期間を設けるようにしたが、そのような期間を設けないようにすることも可能であるし、3以上の期間を設けるようにすることも可能である。同様に、鍵テーブルの各エントリに登録する復号鍵の数も、1つだけとしたり、3以上とすることが可能である。

【0103】

また、本実施の形態では、データを、DVBの規格に準拠する形で配信するようにしたが、データの配信は、DVBの規格に準拠しない形で行うことも可能である。

【0104】

次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや、1チップのマイクロコンピュータ等にインストールされる。

【0105】

そこで、図7は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0106】

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク105やROM103に予め記録しておくことができる。

【0107】

あるいはまた、プログラムは、フロッピーディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体111に、一時的あるいは永続的に格納(記録)しておくことができる。このようなリムーバブル記録媒体111は、いわゆるパッケージソフトウェアとして提供することができる。

【0108】

なお、プログラムは、上述したようなリムーバブル記録媒体111からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部108で受信し、内蔵するハードディスク105にインストールすることができる。

【0109】

コンピュータは、CPU(Central Processing Unit)102を内蔵している。CPU 102には、バス101を介して、入出力インタフェース110が接続されており、CPU102は、入出力インタフェース110を介して、ユーザによって、キーボードやマウス等で構成される入力部107が操作されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)103に格納されているプログラムを実行する。あるいは、また、CPU102は、ハードディスク105に格納されているプログラム、衛星若しくはネットワークから転送され、通信部108で受信されてハードディスク105にインストールされたプログラム、またはドライブ109に装着されたリムーバブル記録媒体111から読み出されてハードディスク105にインストールされたプログラムを、RAM(Random Access Memory)104にロードして実行する。これにより、CPU102は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU102は、その処理結果を、必要に応じて、例えば、入出力インタフェース110を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部106から出力、あるいは、通信部108から送信、さらには、ハードディスク105に記録等させる。

【0110】

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0111】

また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0112】

【発明の効果】

本発明のデータ処理装置およびデータ処理方法、並びに記録媒体によれば、宛先と、その宛先が登録されているエントリが有効であるかどうかを表すエントリ有効情報とが登録されているエントリを有するテーブルを参照することで、そのテーブルから、データブロックの宛先に一致する宛先を有するエントリが、注目エントリとして検索される。そして、注目エントリに登録されたエントリ有効情報に基づいて、注目エントリが有効かどうか判定され、その判定結果に基づいて、データブロックに配置されたデータの出力が制御される。従って、データを正常に取得することのできるユーザを、容易に制限することが可能となる。

【図面の簡単な説明】

【図 1】

本発明を適用した放送システムの一実施の形態の構成例を示すブロック図である。

【図 2】

図 1 の送信システム 1 の処理を説明するためのフローチャートである。

【図 3】

セクションとセクションヘッダのフォーマットを示す図である。

【図 4】

図 1 の受信装置 2 2 の構成例を示すブロック図である。

【図 5】

鍵テーブルを示す図である。

【図 6】

図 4 の受信装置 2 2 の処理を説明するためのフローチャートである。

【図 7】

本発明を適用したコンピュータの一実施の形態の構成例を示すブロック図である。

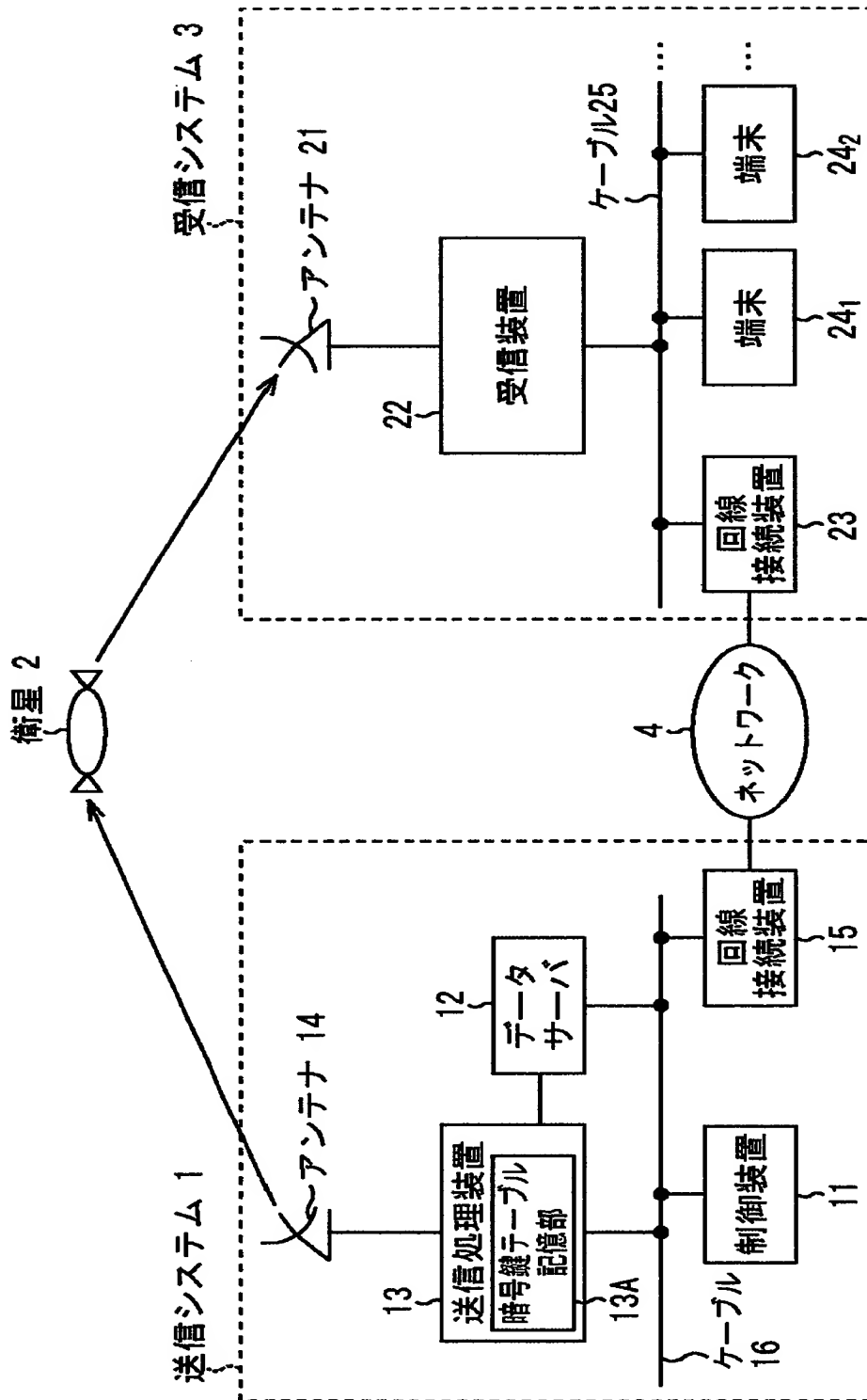
【符号の説明】

1 送信システム, 2 衛星, 3 受信システム, 4 ネットワーク,
1 1 制御装置, 1 2 データサーバ, 1 3 送信処理装置, 1 3 A
暗号鍵テーブル記憶部, 1 4 アンテナ, 1 5 回線接続装置, 1 6 ケ

ーブル, 21 アンテナ, 22 受信装置, 23 回線接続装置, 24
 1, 24₂ 端末, 31 フロントエンド部, 32 デマルチプレクサ, 3
 3 復号LSI, 34 CPU, 35 I/F, 41 フィルタ, 42
 復号器, 43 鍵テーブル記憶部, 44 チェッカ, 45 FIFOバ
 ッファ, 101 バス, 102 CPU, 103 ROM, 104 RAM,
 105 ハードディスク, 106 出力部, 107 入力部, 108 通
 信部, 109 ドライブ, 110 入出力インタフェース, 111 リム
 ーバブル記録媒体

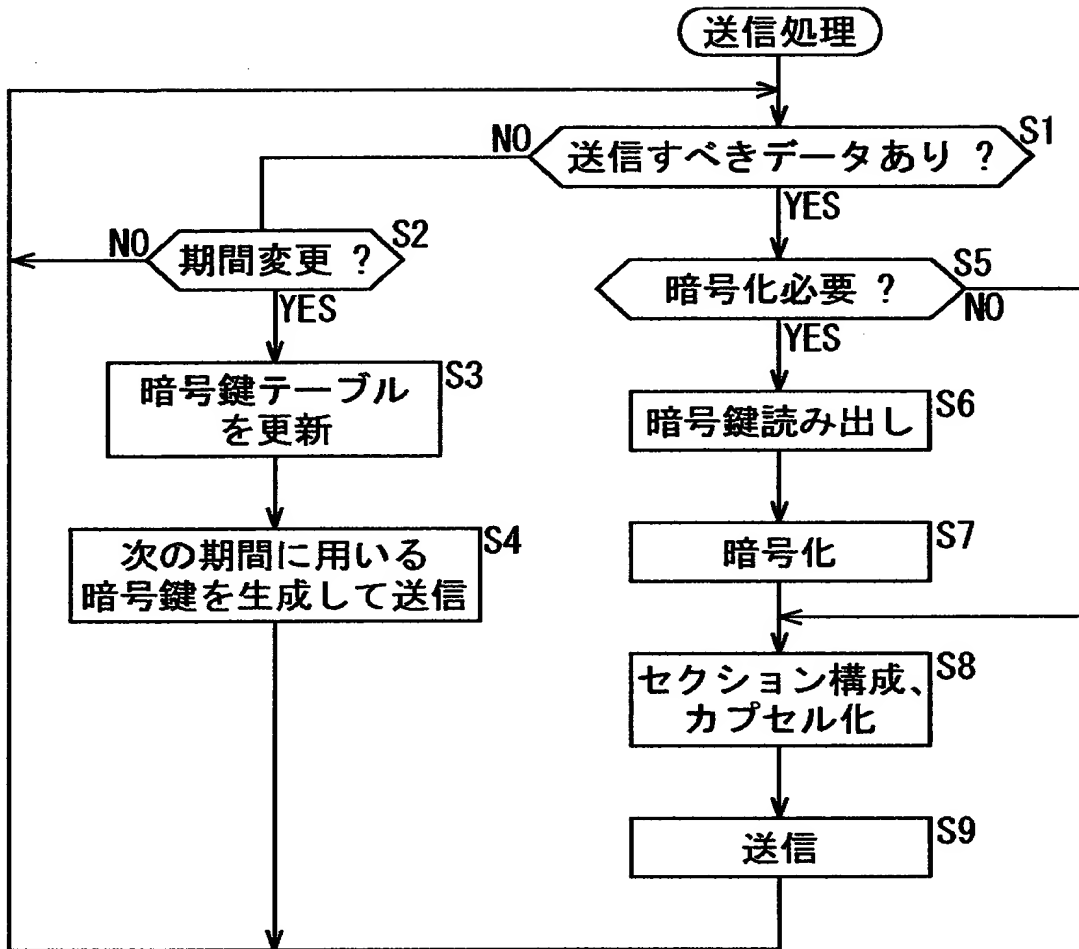
【書類名】 図面

【図 1】

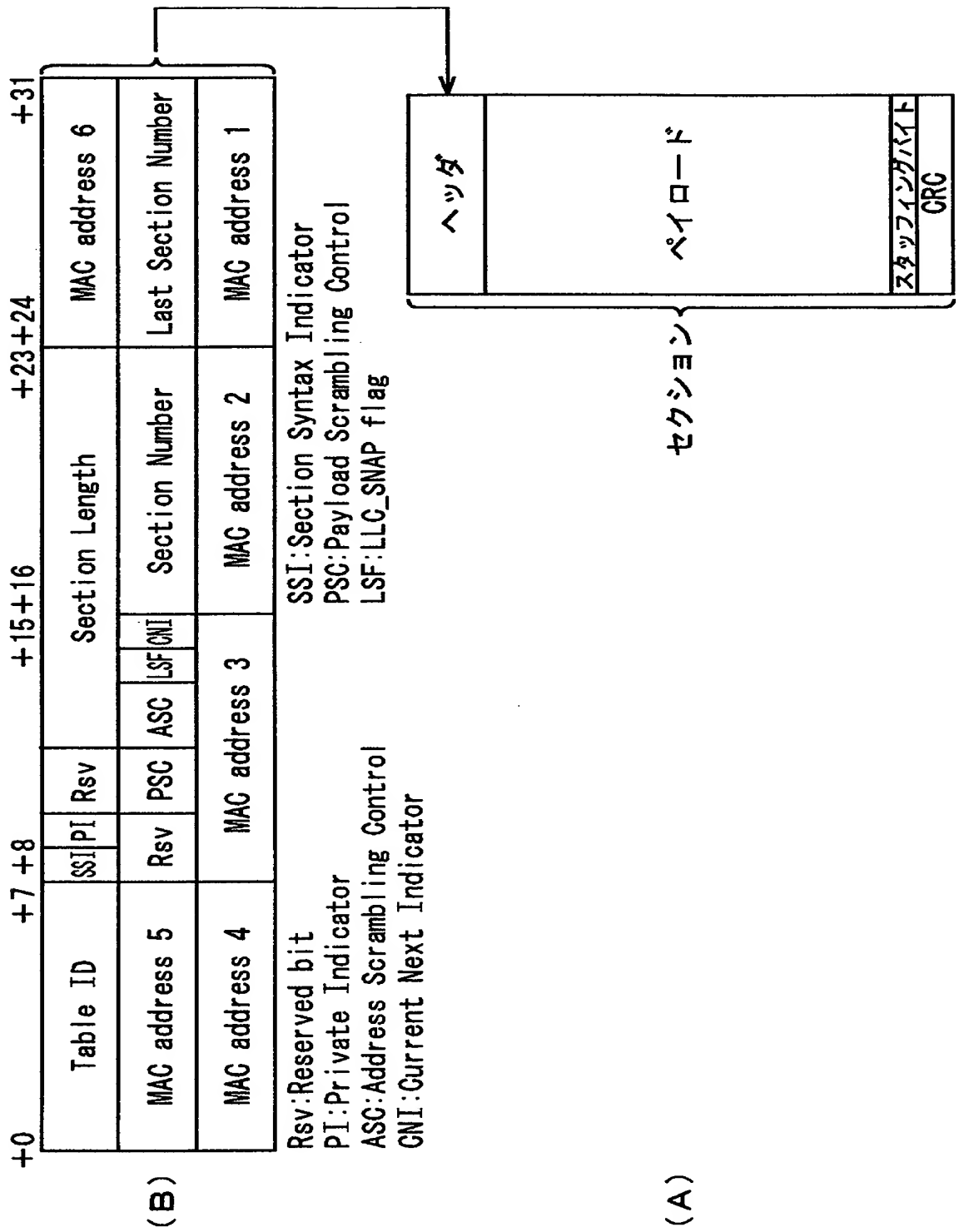


放送システム

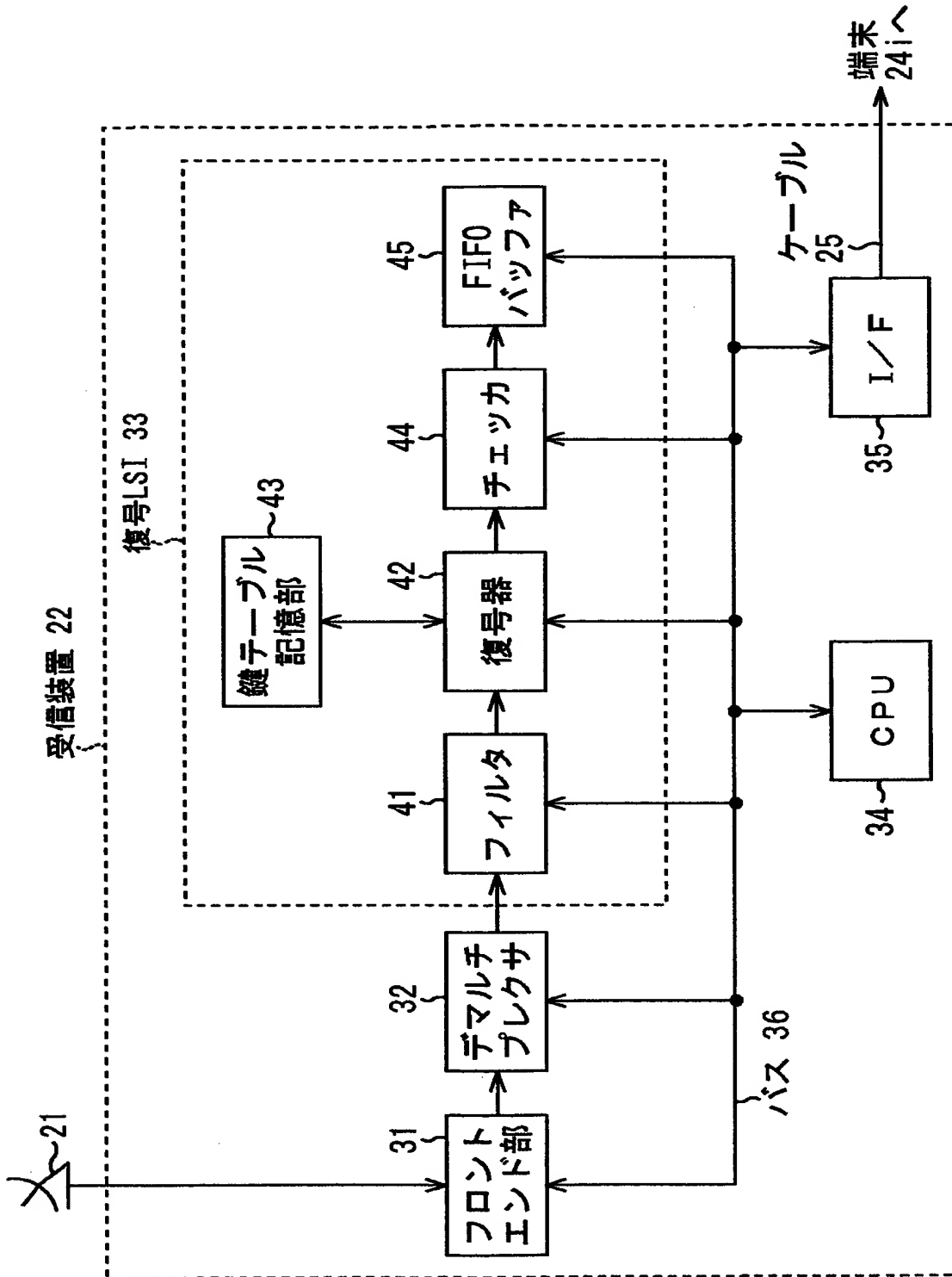
【図 2】



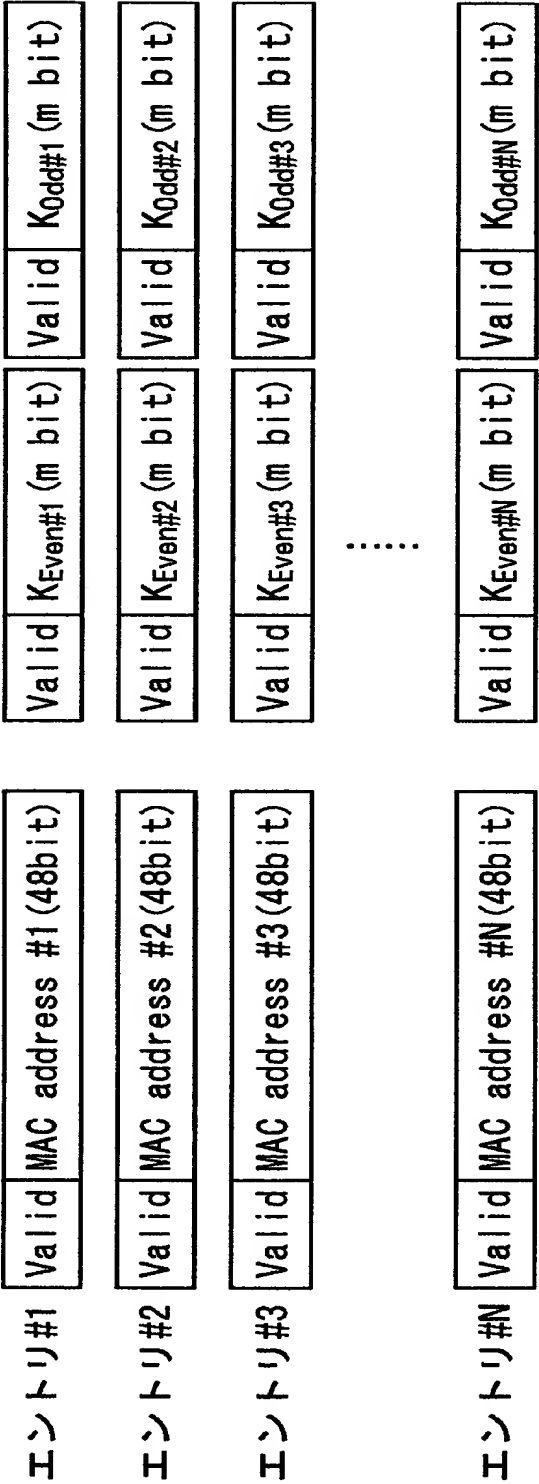
【図 3】



【図 4】

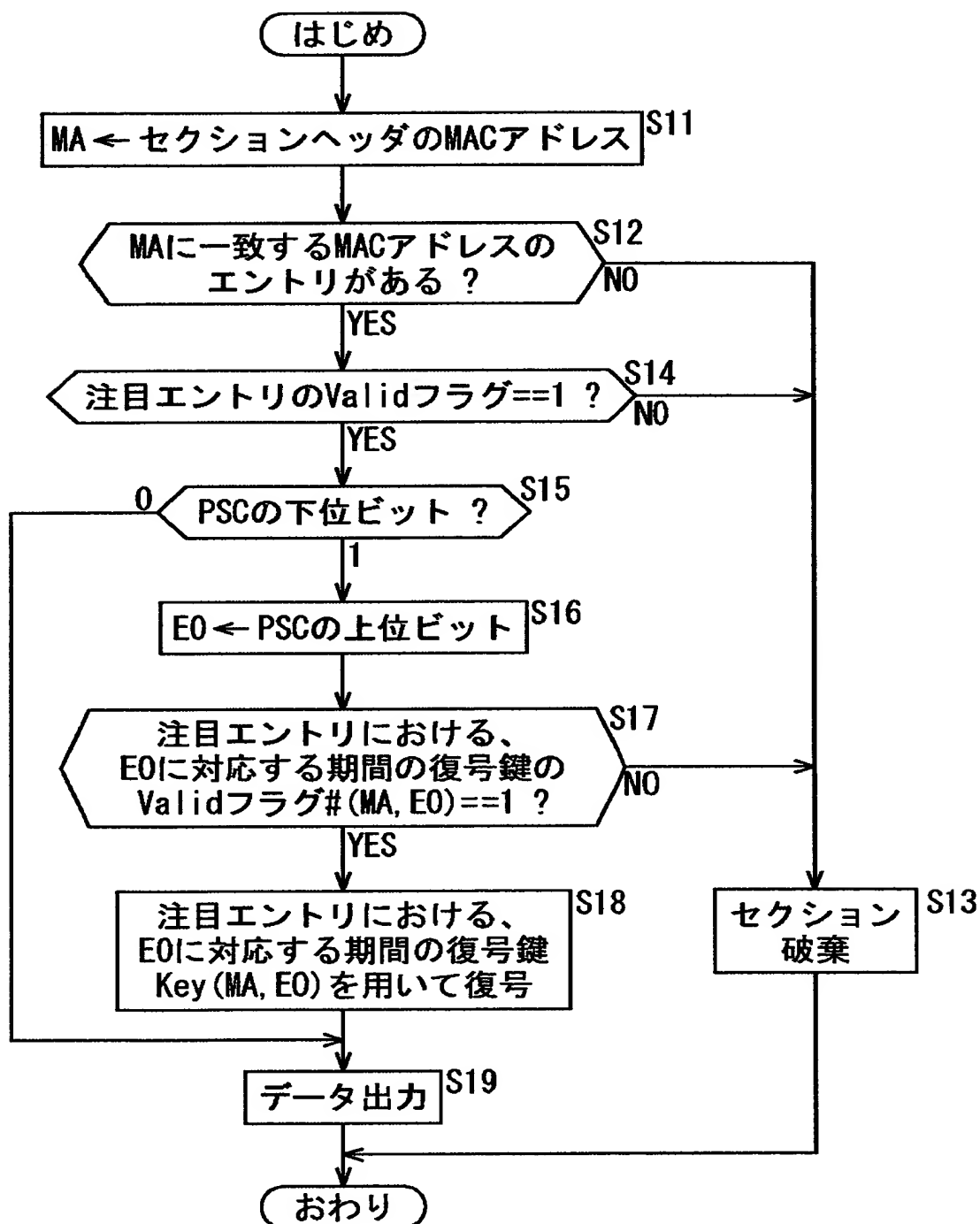


【図 5】

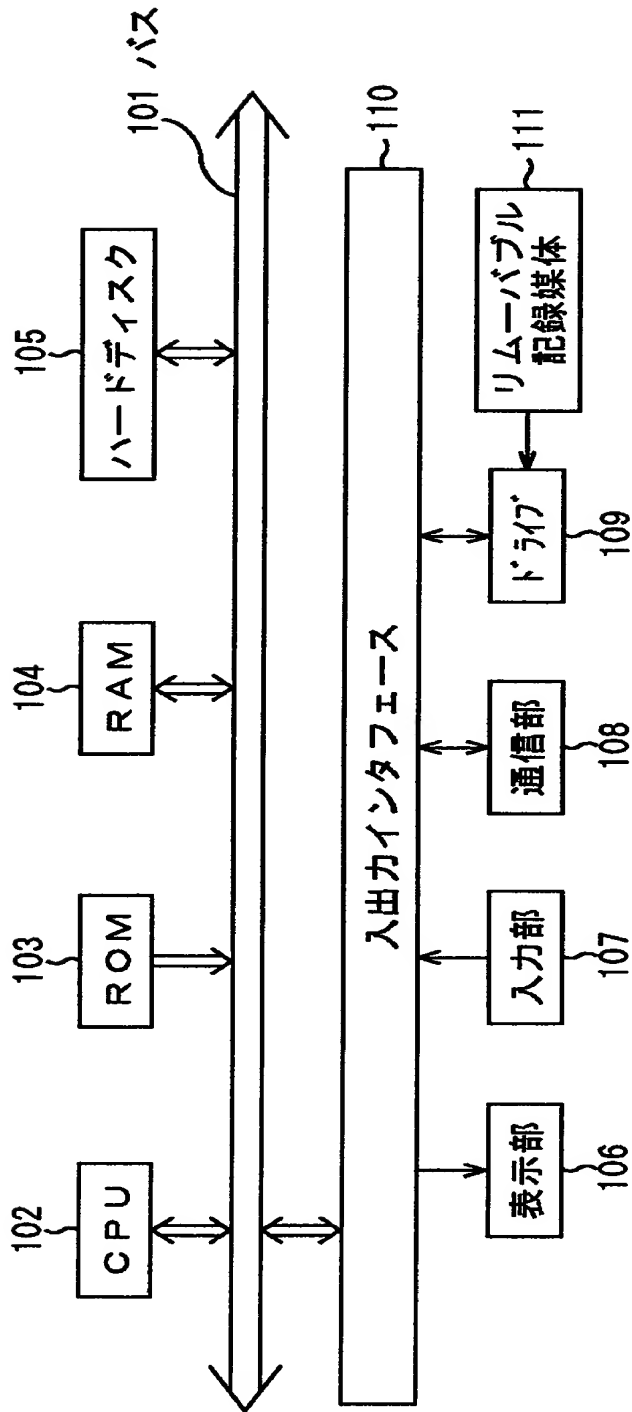


鍵データベース

【図 6】



【図 7】



コンピュータ

【書類名】 要約書

【要約】

【課題】 データを正常に取得することのできるユーザを、容易に制限する。

【解決手段】 鍵テーブルの各エントリ # i には、端末の MAC アドレス $MAC_{address\#i}$ と、その MAC アドレスに割り当てられている復号鍵 $K_{Even\#i}$ および $K_{Odd\#i}$ とが対応付けられて登録されている。さらに、各エントリ # i の MAC アドレス $MAC_{address\#i}$ には、そのエントリ # i が有効であるかどうかを表す Valid ビットが付加されている。この場合において、受信されたセクションのセクションヘッダに配置されているのと同じの MAC アドレスが、鍵テーブルから検索され、その MAC アドレスのエントリが有効かどうか、Valid ビットに基づいて判定される。そして、エントリが有効である場合のみ、セクションのペイロードに配置されたデータが復号されて出力される。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社

THIS PAGE BLANK (USPTO)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)